Security Assurance Levels: A Vector Approach

Jim Gilsinn
National Institute of Standards & Technology (NIST)
Engineering Laboratory (EL)

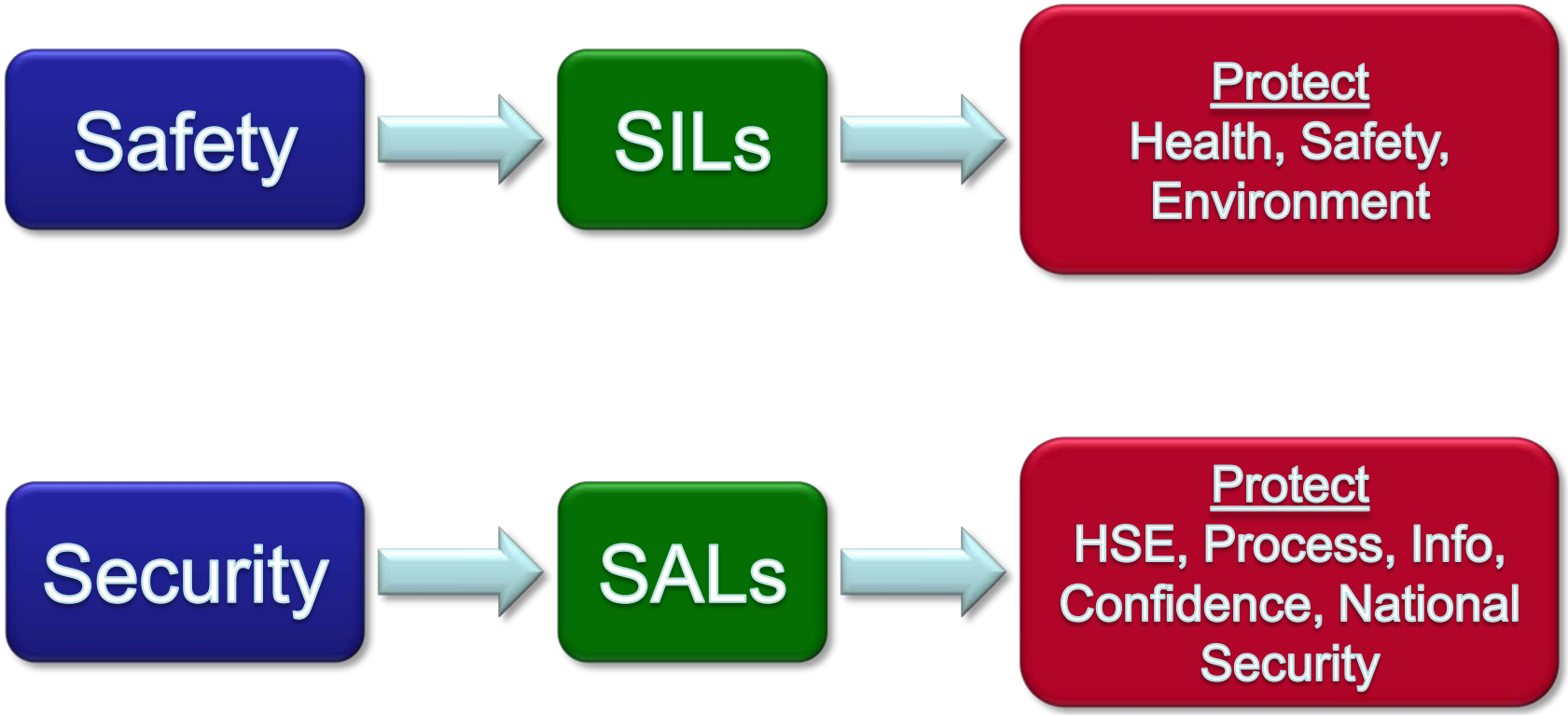
Ragnar Schierholz
ABB Corporate Research

ICSJWG 2010 Fall Conference

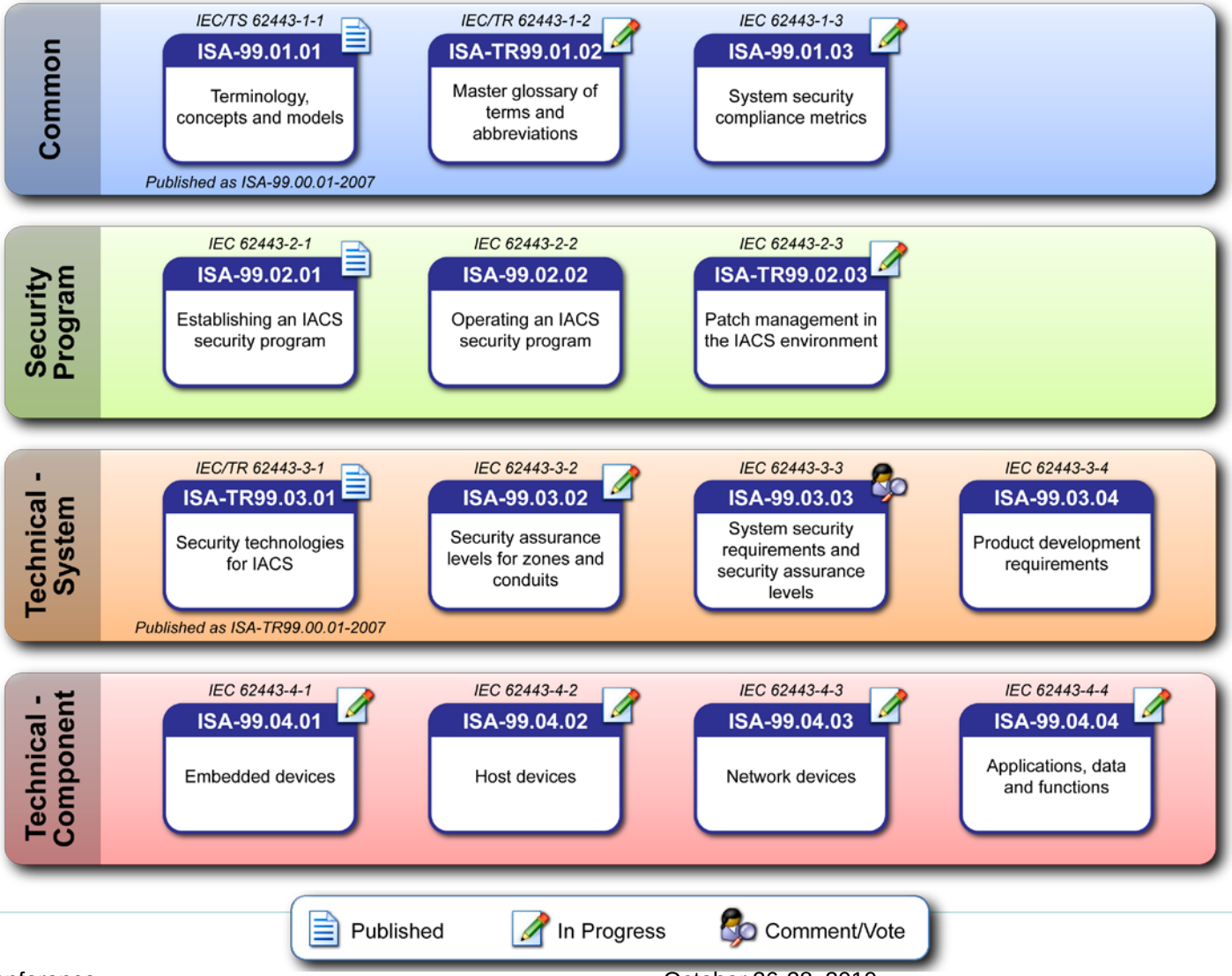
Overview

- Introduction
- ISA-99 Document Series
- Types of SALs
- Using SALs
- Level Definitions
- Foundational Requirements
- Vector Format
- Questions

Introduction



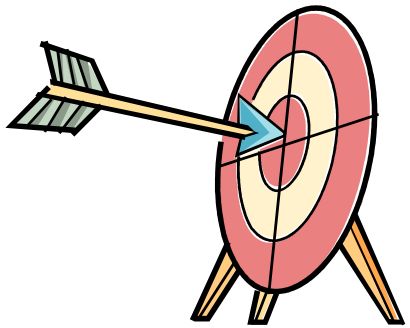
ISA-99 Document Series



Status current as of October 2010

Types of SALs

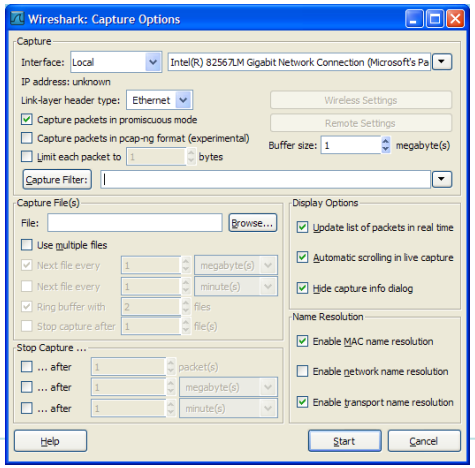
- Target SALs



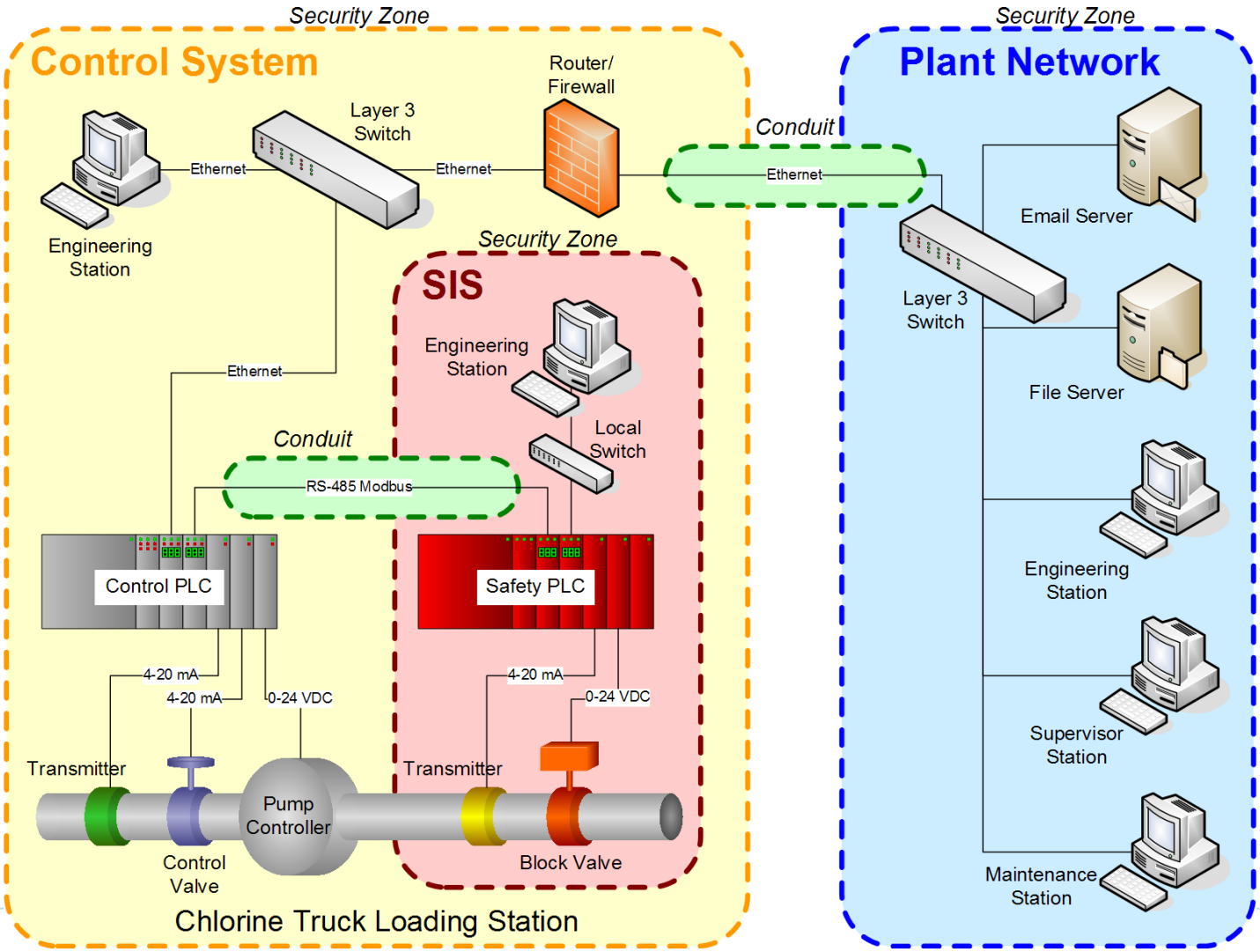
- Designed SALs

- Achieved SALs

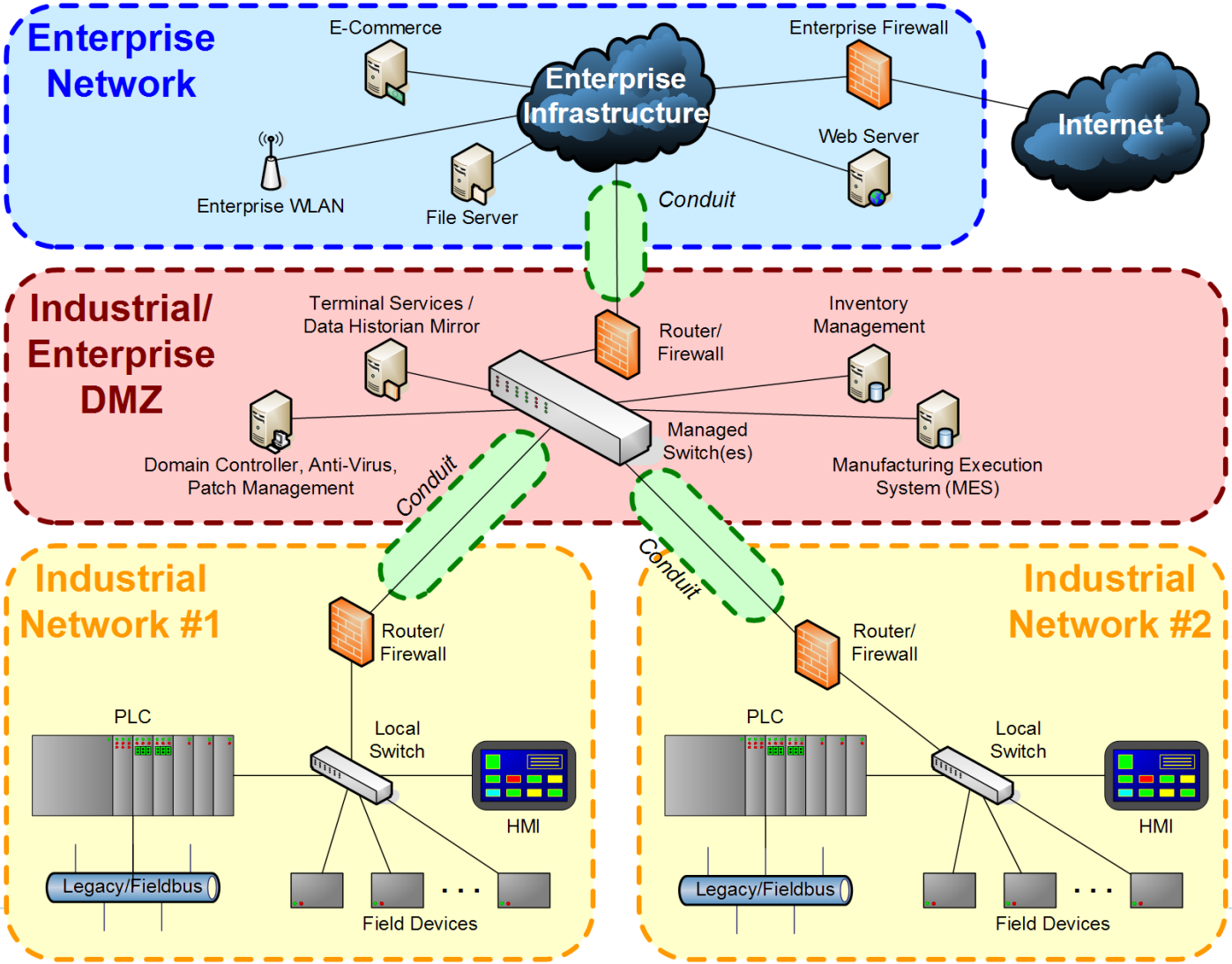
- Capability SALs



Using SALs: Process Example



Using SALs: Manufacturing Example



Level Definitions

1. Casual or Coincidental Violation
2. Intentional Violation Using Simple Means
3. Intentional Violation Using Sophisticated Means
4. Intentional Violation Using Sophisticated Means & Extended Resources

Foundational Requirements

AC Access Control

UC Use Control

RA Resource Availability

DI Data Integrity

TRE Timely Response to an Event

RDF Restrict Data Flow

DC Data Confidentiality

SAL Vector Format

$$SAL\text{-}?([FR,]domain) = \{AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA\}$$

- Examples
  - SAL-T(Control System Zone) = {2 2 0 1 3 1 3}
  - SAL-C(Engineering Workstation) = {3 3 2 3 0 0 1}
  - SAL-C(RA, Safety PLC) = 4
- Definition & usage still under development

Contact Information

- Jim Gilsinn
  - National Institute of Standards & Technology (NIST)
  - +1-301-975-3865
  - james.gilsinn@nist.gov
- Ragnar Schierholz
  - ABB Corporate Research
  - +41 (58) 5868297
  - ragnar.schierholz@ch.abb.com